National Computer Board

CERT-MU

CERT-MU Security Alert

COVID-19: Watch out for the Vulnerabilities

Issue Date: 30 March 2020

Description:

As the coronavirus pandemic continues to disrupt global health, economic, political and social systems, there is another unseen threat rising in the digital space: the risk of cyberattacks that prey on our increased reliance on digital tools and the uncertainty of the crisis. Businesses and public-sector organisations are increasingly offering or enforcing work from home policies, and social interactions are rapidly becoming confined to video calls, social media posts and chat programmes. Many governments are disseminating information via digital means. For example,

Mauritius has launched an app known as "Besafe Moris" as a mode of disseminating information regarding the COVID-19 in the country. In today's unprecedented context, a cyberattack that deprives organisations or families of access to their devices, data or the internet could be devastating.

The speed at which organisations are being forced to respond to the unfolding COVID-19 health crisis could be leaving many of them vulnerable to attack by threat actors rushing to exploit the situation. Over the past few weeks, security vendors and researchers have reported an increasing number of malicious activities tied to COVID-19. Predictably, a lot of the activity has involved phishing and social-engineering campaigns where COVID-19 has been used as a thematic lure to get people to click on malicious attachments and links in emails or to download malware on mobile and other devices. There have also been reports about account takeover and business email compromise activity, a growth in domains serving up drive-by malware, and attempts to exploit virtual private networks (VPNs) and other remote access tools. The danger posed by these threats has been aggravated by new requirements for "social distancing" and the resulting push by many organisations to widen or implement telework capabilities for their workforce. The sudden COVID-19-related surge in the use of videoconferencing, remote access, and VPN services, especially at organisations that have not used them is giving attackers more opportunities to conduct cyber-attacks.

CERT-MU recommends organisations to remain vigilant and ensure that they are engaged in cyber defense best practices, including increased monitoring of network logs, reminding employees to practice phishing awareness and ensuring that servers and critical systems are patched for all known security vulnerabilities.

Critical Vulnerabilities

The vulnerabilities related to telework are of particular concern during the current pandemic. As organisations rush to make more infrastructure available to remote users, configuration errors may be made and unpatched software may be deployed. CERT-MU recommends applying patches and mitigations for critical vulnerabilities that have been reported during the weeks of 16 to 27 March 2020 as they may be exploited if remain unpatched:

Vulnerability Name	Description	Affected Systems	Workarounds
Enterprise VPN Security	• As organisations use VPNs for telework, more vulnerabilities are being found and targeted by malicious cyber actors. • As VPNs are 24/7, organisations are less likely to keep them updated with the latest security updates and patches. • Malicious cyber actors may increase phishing emails targeting teleworkers to steal their usernames and passwords. • Organisations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks. • Organisations may have a limited number of VPN connections, after which point no other employee can telework. With decreased availability, critical business operations may suffer, including IT security personnel's ability to perform cybersecurity tasks.	Enterprise Virtual Private Network	• Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations. • Alert employees to an expected increase in phishing attempts. • Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery • Implementation of Multi-Factor Authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords. • Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications such as rate limiting to prioritize users that will require higher bandwidths.

			More information about VPN security is available on: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
Microsoft Windows Remote Code Execution Vulnerability	A vulnerability has been identified in Microsoft Windows which could be exploited by remote user to trigger remote code execution on the targeted system.	• Windows 7, 32 and 64-bit • Windows 8.1, 32 and 64-bit • Windows 10, 32 and 64-bit • Windows Server 2008 • Windows Server 2012 • Windows Server 2016 • Windows Server 2019	Users are advised to apply updates. More information is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200006
Adobe Creative Cloud Desktop Application Data Manipulation Vulnerability	A vulnerability was identified in Adobe Creative Cloud Desktop Application, which could be exploited by remote attacker to trigger data manipulation on the targeted system.	• Creative Cloud Desktop Application 5.0 and earlier versions	Users are advised to upgrade to Creative Cloud Desktop Application 5.1. More information is available on: https://helpx.adobe.com/security/products/creative-cloud/apsb20-11.html
IBM WebSphere Application Multiple Vulnerabilities	Multiple vulnerabilities were identified in IBM WebSphere Application Server which could be exploited by a remote attacker to trigger denial of service condition, remote code execution, obtain sensitive information, cross-site scripting and bypass security restriction on the targeted system.	• IBM WebSphere Application Server Liberty 17.0.0.3 - 20.0.0.1 • IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0	Users are advised to apply updates. More information is available on: https://www.ibm.com/support/pages/node/6113998
Apple Products Multiple Vulnerabilities	Multiple vulnerabilities were identified in Apple products which could be exploited by remote attacker to trigger denial of service condition, elevation of privilege, remote code execution, disclose sensitive information, cross-	• iOS prior to 13.4 • iPadOS prior to 13.4 • iTunes for Windows prior to 12.10.5 • macOS Catalina 10.15.3 and prior versions	Users are advised to apply updates. More information is available on: https://support.apple.com/en-us/HT201222

	site scripting and bypass security restriction on the targeted system.	• macOS High Sierra 10.13.6 and prior versions • macOS Mojave 10.14.6 and prior versions • Safari prior to 13.1 • tvOS prior to 13.4 • watchOS prior to 6.2 • Xcode prior to 11.4	
Multiple Vulnerabilities in Microsoft Azure DevOps and Team Foundation Server	Multiple vulnerabilities have been identified in Microsoft Azure DevOps and Team Foundation Server which could allow remote attackers to perform cross-site scripting, execute malicious code and escalate privileges on the target system.	• Azure DevOps Server 2019 Update 1 • Azure DevOps Server 2019 Update 1.1 • Azure DevOps Server 2019.0.1 • Team Foundation Server 2018 Update 1.2 • Team Foundation Server 2018 Update 3.2 • Team Foundation Server 2017 Update 3.1	Users are advised to apply updates. More information is available on: https://portal.msrc.microsoft.com/en-us/security-guidance
Multiple Vulnerabilities in Microsoft Visual Studio	Multiple Vulnerabilities have been identified in Microsoft Visual Studio, which could be exploited by remote attackers to cause a denial of service attack, elevation of privilege and spoofing on the targeted system.	• Microsoft Visual Studio 2019 version 16.0 • Microsoft Visual Studio 2019 version 16.4 • Microsoft Visual Studio 2017 version 15.9 • Microsoft Visual Studio 2015 Update 3	Users are advised to apply updates. More information is available on: https://portal.msrc.microsoft.com/en-us/security-guidance

The Computer Emergency Response Team of Mauritius is working to ensure cyber threat preparedness in the country where it is fighting against the COVID-19. With COVID-19-related threats escalating on the cyber front and the move to remote access technology as a key means of communication, the need to enforce cybersecurity is vital for organisations to deliver essential business operations. Hence, organisations and employees need to be prepared, and adopt a heightened state of cybersecurity to enhance their cybersecurity postures and stay cyber-safe while telecommuting.

CERT-MU recommends the following measures that organisations and employees can take to enhance your cybersecurity posture:

Organisations:

- Make sure that the VPN, network infrastructure devices, endpoint devices, and other remote access systems are updated with the latest patches and security configurations, as well as anti-virus signatures. Where possible, implement Multi-Factor Authentication (MFA) on all VPN connections.

- Stay up to date and follow the good practices guide recommended by solution providers to keep systems secure.

- Organisations may also consider restricting remote access to sensitive systems where practical. Closely monitor authentication logs for remote services and look out for suspicious account behaviour or activities across systems, for example, if one account is logged into multiple systems simultaneously.

- Organisations need to provide regular reminders to employees about cyber threats and preventive tips so that their awareness is heightened.

- Reiterate the Acceptable Use Policy if needed, and enforce strict security policies such as the frequency of change and strength of passwords, downloading of applications on company-issued devices and usage of USB devices.

Employees:

- Always stay vigilant, especially if you receive a COVID-19 themed e-mail that requests for sensitive information or requires financial payments.

- Use a secure Wi-Fi network, and always make sure to send important and sensitive information over Virtual Private Network (VPN).

- If you are working from home, you should also ensure that the home router is secure by changing the default password, and checking that security settings are set to enable automatic updates, disable remote access, and disable Universal Plug and Play (UPnP).

- Alert your IT team if you detect any unusual or suspicious activities on your terminal, or if you have clicked on any phishing links.

- After a teleconferencing session, it is a good practice to mute the microphone and cover the camera. Lock the screen if you are stepping away from your terminal or taking a break. When you are done for the day, you should also shut down your terminals so that any updates that are pushed down to the terminals can be installed properly upon restart.